1   S P E C I F I C A T I O N

2   METHOD AND SYSTEM FOR CONFIRMING PROPER RECEIPT OF
3   E-MAIL TRANSMITTED VIA A COMMUNICATIONS NETWORK

4   **BACKGROUND OF THE INVENTION**

5   This is a continuation-in-part of Application No.

6   09/460,531, filed September 15, 1999.

7   The field of the invention generally relates to receipt

8   confirmation methods and systems. The invention relates more

9   particularly to a method and system for confirming proper receipt

10   of electronic mail ("e-mail") intended by a sending party for

11   transmission to a target e-mail address of a target party. The

12   e-mail is properly or improperly delivered to a recipient e-mail

13   address, wherein information associated with the recipient e-mail

14   address, such as the identity of an accessing party, is

15   automatically discovered and transmitted to the sending party

16   when a designated access event is triggered by an accessing

17   party.

18   Many significant developments have been made in recent years

19   in a variety of communications mediums. In particular, the

20   development of the Internet, localized intranets, and similarly

21   network-based communications has made inter-connectivity and

22   networking possible on both a local as well as global scale.

23   Moreover, with the growth of online communications networks,

24   various devices and methods have been developed to facilitate as

1

1 well as promote online communication and means for conducting

2 business. One recent development has been the creation of e-mail

3 which allows users to electronically send and receive various

4 forms of analog or digitized data, including text, graphics,

5 video, sounds, etc. almost anywhere, and virtually

6 instantaneously. In recent years, e-mail has grown tremendously

7 in popularity, and has gained widespread use throughout the

8 world.

9   Unfortunately, however, e-mail does not yet afford users the

10 same sense of security and reliability in delivery as other more

11 traditional communications mediums, such as mail delivered by the

12 postal system. It is often frustrating to find that an e-mail

13 message thought to be properly delivered, was never received by

14 the intended target recipient because of an unknown system error

15 or malfunction. In such a case, the e-mail may even have been

16 delivered to an unintended party as a result of the system error.

17 Additionally, in the case where e-mail is properly delivered to

18 the target party's e-mail address, actual receipt and notice by

19 the intended target party may have been prevented due to access

20 by unauthorized individuals or other unforeseen circumstances.

21 These scenarios are particularly devastating when important

22 documents and materials transmitted over the Internet are

23 involved and are never received. Especially in these cases,

24 therefore, it is essential that the sending party verify and

25 receive confirmation that the e-mail was properly delivered to

1   the intended e-mail address, and that the intended target party

2   actually received and was notified of the e-mail delivery.

3   Traditionally, receipt confirmation of documents and

4   materials sent via the postal system has been through signature

5   request on a paper return receipt at the point of physical

6   delivery. This technique, often used by mail service delivery

7   agents, confirms completed delivery at the target address or

8   location and is intended to provide the sender with a measure of

9   security and some evidence that the sent materials were in fact

10   delivered to the proper address. However, the disadvantage of

11   this traditional method of receipt confirmation is that it can be

12   time-consuming, ineffective, and disproportionately expensive,

13   especially in light of the expanding prevalence of the Internet

14   as a global communications medium. Moreover, while a recipient's

15   signature is typically required upon delivery, the signature

16   alone does not provide dispositive confirmation that an intended

17   target individual actually received or was notified of the

18   delivery, particularly in a household or place of business with

19   many people.

20   One particular method of receipt confirmation has been

21   widely used on the Internet, particularly in the electronic

22   greeting card industry. For example, when an electronic greeting

23   card is chosen from a website by a sending party for delivery to

24   a target recipient, an e-mail message is typically sent to the

25   target recipient in lieu of the greeting card itself. The e-mail

3

1   message notifies the target recipient that an electronic greeting

2   card awaits him/her at the website. When the target recipient

3   accesses the greeting card at the designated website, a

4   confirmation receipt e-mail message is automatically generated by

5   the greeting card service and sent to the sending party who has

6   previously provided his return e-mail address. While this

7   particular method provides a certain level of reliability that

8   the intended target recipient accessed and viewed the card, it is

9   uncertain that the target recipient will acknowledge the greeting

10   card at all by actually visiting the designated Internet website.

11   Only with the target recipient's cooperation would a receipt

12   confirmation be generated and sent back to the sending party.

13   Additionally, because this form of Internet delivery confirmation

14   requires the participation of a third party service provider

15   functioning as an intermediary, delivery and confirmation is

16   indirect and relatively inefficient, especially since direct

17   communication and delivery is readily available to all e-mail

18   users. Moreover, this method of receipt confirmation also does

19   not positively identify the individual or entity that actually

20   accessed the e-mail or the location (e-mail account or geographic

21   address) from which it was accessed.

22   Receipt confirmation of directly transmitted e-mail

23   deliveries between e-mail users is presently possible by manual

24   return e-mail confirmation. This typically requires a series of

25   additional actions to be taken by the target recipient, i.e. by

1 independently writing a separate confirmation e-mail. Again,

2 however, the success of this method requires the participation

3 and cooperation of the recipient to confirm receipt of a

4 delivered e-mail. Without the recipient party's cooperation, it

5 is uncertain in most cases whether a particular e-mail was

6 properly delivered to the correct e-mail address, or whether the

7 proper target party accessed or was notified of the e-mail. Even

8 in situations where e-mail is properly delivered to a target

9 party's "inbox," i.e. a logical destination where new e-mail is

10 placed prior to opening, there is typically no evidence to

11 indicate that the target party actually opened to view the e-mail

12 or confirm notice. The target party may discriminately choose to

13 open and view certain e-mails received while never opening and

14 examining the contents of others. This would be particularly

15 problematic in situations where proof of service with notice is

16 required, such as service of jury duty summons, or other legal

17 and court documents. It would also pose a problem in other

18 situations which are unlikely to elicit cooperation from the

19 intended recipient.

20   In summary, therefore, it would be advantageous to afford

21 the sending party a means for confirming receipt of the e-mail

22 which is substantially beyond the control of the recipient party.

23 Furthermore, it would be advantageous to actively determine the

24 identity of the recipient individual actually receiving and/or

25 given notice of the e-mail, as well as other actively discovered

5

1   information indicative of proper delivery which is found on the

2   recipient computer system of the recipient individual.

BRIEF SUMMARY OF THE INVENTION

4   It is therefore an object of the present invention to

5   provide a prompt and reliable method and system for confirming

6   proper receipt of e-mail transmitted over a communications

7   network, such as the Internet.

8   It is a further object of the present invention to provide a

9   prompt and reliable method and system which affords a party

10 sending e-mail a greater sense of security that an e-mail was in

11 fact delivered to and accessed by a target party by return-

12 receiving a confirmation of receipt notice which confirms or

13 denies actual notice and receipt by the intended target party of

14 the delivered e-mail.

15   It is a still further object of the present invention to

16 actively and positively identify the individual who accesses the

17 delivered e-mail and the location from which it was accessed by

18 discovering recipient information related to a recipient e-mail

19 address, such as identity information of the accessing party as

20 well as the recipient e-mail address.

21   The present invention is for a method and system for

22 confirming proper receipt of e-mail transmitted over a

23 communications network. In a first preferred embodiment, the

24 present invention is a method comprising the following steps.

6

1   First, an e-mail file is obtained by a sending party and intended

2   for transmission to a target e-mail address associated with a

3   target party. Next, the e-mail file is electronically

4   transmitted from a first computer which is connected to the

5   communications network and associated with the sending party.

6   Next, the e-mail is properly or improperly delivered to a

7   recipient e-mail address associated with a second computer

8   connected to the communications network. Next, a designated

9   access event is detected when it is triggered by the accessing

10 party. The access event is generally associated with e-mail

11 retrieval from the recipient e-mail address, and can include, for

12 example, when the accessing party gains access to the second

13 computer or the recipient e-mail address, or when the accessing

14 party opens the e-mail file itself. In any event, the following

15 steps are automatically executed upon detection of the access

16 event. They include: (1) providing notice of the delivered e-

17 mail file to the accessing party, (2) discovering recipient data

18 which is generally associated with the recipient e-mail address,

19 (3) generating a confirmation of receipt notice containing the

20 discovered recipient data, and (4) electronically transmitting

21 the confirmation of receipt notice from the second computer to a

22 return e-mail address associated with the sending party.

23 Preferably, the discovering step includes access event data

24 associated with the designated access event, such as identity

25 information of the accessing party. Moreover, the discovering

7

1 step preferably also includes retrieving an accessing party data

2 file containing accessing party identity information which was

3 previously obtained from the accessing party as a requisite

4 condition for either 1) accessing the second computer or the

5 recipient e-mail address, or 2) operating a remote user computer

6 connected to the second computer via the communications network.

7 And finally, the recipient data contained in the confirmation of

8 receipt notice is compared with intended delivery information

9 associated with the intended target party. In this manner, the

10 sending party may determine whether the e-mail file was properly

11 delivered or not.

12   In a second preferred embodiment of the present invention,

13 the general method discussed above further comprises the step of

14 obtaining access event data of attendant conditions of the access

15 event upon detection of the access event. Furthermore, the steps

16 of providing notice of the delivered e-mail file, generating the

17 confirmation of receipt notice, and electronically transmitting

18 the confirmation of receipt notice are all conditioned upon first

19 obtaining the access event data. Preferably, the access event

20 data is obtained by interactively requesting and receiving input

21 from the accessing party.

22   And in a still third preferred embodiment of the present

23 invention, a system is provided for confirming proper receipt of

24 e-mail. The system comprises an e-mail file intended by a

25 sending party for electronic transmission to a target e-mail

1   address associated with a target party. Additionally, the system

2   includes a first computer connected to the communications network

3   and from which the sending party may electronically transmit the

4   e-mail file. A second computer is also included which is

5   connected to the communications network and associated with a

6   recipient e-mail address. The second computer has a data storage

7   location for storably receiving the e-mail file thereon upon

8   delivery to the recipient e-mail address. The system also

9   comprises first executable software means for detecting a

10   designated access event which is triggered by an accessing party

11   and is generally associated with e-mail retrieval from the

12   recipient e-mail address. Additionally, a second executable

13   software means of the system provides notice of the delivered e-

14   mail file to the accessing party. The system also has third

15   executable software means for discovering recipient data which is

16   associated with the recipient e-mail address. For example, the

17   recipient data may include pre-recorded registered recipient

18   information resident in the second computer, or identity

19   information of an accessing party actually being notified of

20   and/or viewing the e-mail file. Additionally, the system

21   includes fourth executable software means for generating a

22   confirmation of receipt notice which contains the recipient data.

23   A fifth executable software means is also included for

24   electronically transmitting the confirmation of receipt notice

25   from the second computer to a return e-mail address associated

9

1   with the sending party. The aforementioned second, third,

2   fourth, and fifth executable software means are all automatically

3   initiated upon occurrence of an access event caused by the

4   accessing party and detected by the first executable software

5   means. In this manner, an examination of the confirmation of

6   receipt notice by the sending party enables the sending party to

7   comparatively determine whether the e-mail was in fact properly

8   delivered to the intended target party.

9   **BRIEF DESCRIPTION OF THE DRAWINGS**

10   FIG. 1 is an overview flowchart depicting the flow of

11   information that occurs between the sending party and the

12   recipient or accessing party in the method and system of

13   confirming proper receipt of e-mail according to the present

14   invention.

15   FIG. 2 is a block diagram of an illustrative e-mail

16   transmission and confirmation of receipt notice retrieval

17   procedure which occurs in the method and system of the present

18   invention.

19   FIG. 3 is an example of a confirmation of receipt notice

20   which confirms proper delivery of the transmitted e-mail file to

21   the correct location and proper access by the intended target

22   party.

23   FIG. 4 is an example of a confirmation of receipt notice

24   which indicates improper delivery of the transmitted e-mail file

1   to the wrong location due to a system or other error and improper

2   access by a non-intended accessing party.

3   FIG. 5 is an overview diagram depicting one embodiment for

4   discovering delivery information associated with the accessing

5   party who actually accesses and is given notice of the delivered

6   e-mail file.

7   **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

8   Referring now to the drawings, FIGS. 1 and 2 together show

9   the information flow that occurs in a method and system 9

10   (hereinafter "system") for confirming proper receipt of e-mail

11   transmitted via a communications network, such as the Internet

12   13.   In particular, FIG. 1 shows an overview flowchart

13   pictorially depicting the general transmission flow of

14   information, i.e. and e-mail file 12, between a sending party 10

15   and a recipient or accessing party 20.   And FIG. 2 shows in block

16   diagram form an illustrative procedure of e-mail transmission and

17   confirmation of receipt notice retrieval which occurs between the

18   sending party 10 and the accessing party 20 according to the

19   present invention.

20   It is initially important to appreciate that the sending

21   party 10 transmitting the e-mail file 12 does so with the intent

22   that it be transmitted to a pre-determined target e-mail address

23   associated with a target party and located on a target computer

24   system.   It is further appreciated, however, that the recipient

1   e-mail address and account to which the e-mail file 12 is

2   actually delivered may or may not be the intended target e-mail

3   address and account. Likewise, the accessing party actually

4   receiving and/or given notice of the transmitted e-mail may or

5   may not be the intended target party. The recipient or accessing

6   party 20 is defined as the individual, whether authorized or not,

7   who actually receives and is given notice of the delivered e-

8   mail, such as by opening and accessing the delivered e-mail. In

9   the case of proper e-mail delivery, the accessing party 20, the

10   recipient e-mail address, and the associated recipient system

11   (14, 21 in FIG. 1) are in fact the intended target party, target

12   e-mail address and target system, respectively, as originally

13   intended by the sending party 10. And in the case of improper

14   delivery, the accessing party 20 is a non-intended third party

15   not designated by the sending party 10 for receipt. It is

16   appreciated that FIGS. 1 and 2 do not make this distinction.

17   Instead, FIGS. 1 and 2 together illustrate the case of general

18   transmission and delivery of e-mail to the recipient e-mail

19   address and account which is associated with and located on a

20   recipient computer system, irrespective of whether the e-mail

21   file was properly or improperly delivered to the recipient e-mail

22   address.

23   As can be seen in FIG. 1, the Internet 13 links together the

24   sending party 10 and the accessing party 20 to enable the

25   transfer of information between them, or with anyone also

12

1   connected to the Internet 13. Although the Internet 13 is used

2   exclusively in the present discussion, it is understood to

3   represent but one form of a communications network. Thus, all

4   references to the Internet 13 are appreciated to generally

5   indicate all forms of communications networks capable of

6   transmitting and receiving data, preferably digital data, which

7   allows users of the network to communicate. In this regard, a

8   communications network includes, but is not limited to, all

9   telecommunications networks such as the Internet, i.e. the World

10   Wide Web and BBS systems, hardwire telephony, wireless networks

11   including cellular and PCS systems, satellite networks, etc.

12   Furthermore, communications networks include localized and

13   regional networks such as intranets and local area network (LAN)

14   systems which interconnect a relatively few number of user

15   systems or terminals, typically by means of a centralized server.

16   As shown in FIG. 1, the sending party 10 first obtains an e-

17   mail file 12 with the intent to send it to a target party using a

18   computer system 11 connected to the Internet 13. The e-mail file

19   12 can be acquired by either creating the e-mail file 12 with a

20   suitable e-mail generating software, or selecting an existing e-

21   mail file 12 for forwarding. An executable attachment file 12',

22   i.e. a relatively small program, may also be created and

23   transmitted along with the e-mail file 12 (see discussion below).

24   It is appreciated that while e-mail such as the e-mail file 12 is

25   most often understood to comprise electronic text messages

1   transmitted via the Internet 13, analogous to a letter delivered

2   by the postal system, it is not limited only to such. The term

3   "e-mail" and "e-mail file" is broadly defined and used herein and

4   in the claims to mean any encoded information containing text,

5   graphics, sound, video, etc. which is transmitted electronically,

6   by analog or digital means, over a communications network,

7   typically the Internet 13. Thus, e-mail can also include all

8   electronic transmissions of analog or digital information which

9   are transmitted and delivered over a communications network, such

10   as file transfer protocol (ftp) transmissions, hypertext transfer

11   protocol (http) transmissions, facsimiles, voice messages, etc.

12   By connecting to the Internet 13, the sending party 10 can

13   electronically transmit the acquired e-mail file 12. As shown by

14   arrows A and B in FIG. 1, the transmission path of the e-mail

15   file 12 to the accessing party 20 depends on where and what type

16   of computer system a registered user of the recipient e-mail

17   address has designated as his recipient computer system, i.e. the

18   destination computer system to which e-mails to the accessing

19   party 20 are delivered and stored. Typically, the registered

20   user effectively designates a particular recipient computer

21   system by choosing from among a wide range of service providers

22   with whom the registered users registers to receive an e-mail

23   address and account.

24   In a first preferred embodiment, as shown in FIG. 1, the

25   recipient computer system is a computer server 14 of a service

14

1   provider capable of processing e-mail for multiple users. For

2   example, the service provider can be an Internet service provider

3   (ISP), such as the online service offered under the trademark

4   "America Online." Alternatively, the service provider can be an

5   e-mail service provider (EMSP), such as the online e-mail service

6   offered under the trademark "Hotmail." Furthermore, the server

7   14 can be a server of an intranet or LAN system which networks a

8   plurality of user terminals (e.g. 19) or workstations together.

9   In this last scenario, it is appreciated that the LAN server can

10   either be a stand alone server system or one of the networked

11   computer workstations or user terminals 19. Moreover, the LAN

12   server can itself be connected to the Internet to centrally

13   provide Internet access to each networked computer workstation or

14   user system.

15   For these server-type recipient computer systems 14, a user

16   account, e.g. a system or e-mail account 16, is typically

17   provided to the registered user. ISPs typically provide their

18   users with a designated user account 16 and an e-mail address

19   associated with the user account, as well as providing access to

20   the Internet. It is notable here that "e-mail address," as used

21   herein and in the claims, is broadly defined as both the address

22   label of the e-mail/user account, and the e-mail/user account

23   itself. Thus "e-mail address" and "e-mail/user account" are used

24   interchangeably throughout this discussion. EMSPs also provide

1   their registered users with a user account 16 and an e-mail

2   address associated with the account, but do not provide access to

3   the Internet. Thus users retrieving e-mail from an EMSP must do

4   so by first connecting to the Internet via an ISP and accessing

5   their designated user accounts. And similar to the servers

6   operated by ISPs or EMSPs, LAN servers also typically provide a

7   user account 16 to the accessing party 20 whereby only authorized

8   personnel gaining access to their user accounts can access shared

9   resources. In all the above situations, incoming e-mail directed

10   to a particular e-mail address, such as the e-mail file 12, are

11   logged and saved under the designated user account 16, which is

12   accessible by password or confidential code entry. Furthermore,

13   to access a user account provided by an ISP or EMSP, the

14   accessing party 20 typically uses a remote user computer 19 to

15   connect directly to the ISP server, or to the EMSP server via an

16   ISP. It is notable here that while the registered user is the

17   original entity having authorized access to the e-mail address,

18   it is the accessing party 20 who gains access to the e-mail

19   address/account, whether authorized or unauthorized, and triggers

20   an access event of the present invention as will be discussed in

21   detail below. Furthermore, the registered user and the accessing

22   party 20 are not mutually exclusive, with one individual capable

23   of assuming both identities.

24   Alternatively, the recipient computer system can be a simple

25   user computer system 21 directly accessible by the accessing

1   party 20. The user system 21 is preferably a personal computer

2   system, which is typically connectable to the Internet via an

3   ISP, or to an intranet as per a LAN system, as discussed above.

4   And e-mail is delivered directly to the user computer. In this

5   scenario, accessing the user computer system 21 and the delivered

6   e-mail requires only that the accessing party 20 power on and

7   directly access the user computer system 21, without having to

8   access a secondary site such as in the server-type systems 14

9   described above.

10   In either case, however, the recipient computer system 14,

11   21 has data storage means 17, 24, typically a hard disk drive,

12   having a storage medium capable of reading and writing data

13   thereon, such as the delivered e-mail 12. Further, the recipient

14   computer system 14, 21 has means for storably receiving e-mail

15   15, 22 on the data storage means 17, 24, which is typically a

16   computer software program. It is notable that the data receiving

17   process for most server 14 and user systems 21 inherently

18   involves writing or storing data, i.e. e-mail, on the data

19   storage means 17, 24 as it is being received.

20   Upon delivery of the e-mail file 12 to the data storage

21   means 17, 24 of the recipient computer system 14, 21, the system

22   9 operates to detect a designated access event 18, 18', 25, 26

23   triggered by the accessing party 20 and generally associated with

24   e-mail retrieval from the recipient e-mail address. Thus the

25   access event may include any action taken by the accessing party

1   20 leading to the opening and viewing of the delivered e-mail,

2   including opening and viewing the delivered e-mail itself. For

3   example, in a first embodiment involving the server-type system

4   14, and denoted by the path indicated by arrow A, the access

5   event can occur upon accessing the server system 14 which is

6   typically accomplished by logging into 18 the user account 16

7   containing the delivered e-mail 12. The access event can also

8   occur upon opening 18' the delivered e-mail file 12 subsequent to

9   logging into 18 the user account, e.g. e-mail account 16 of an

10   EMSP. Typically, because logging into a user account 16 requires

11   a password or confidential access code, a sufficient degree of

12   security is generally provided to ensure that an individual

13   actually logging on is in fact the accessing party 20. However,

14   it should be noted that alternative means of identity

15   verification upon access, such as fingerprint, DNA, retina scan

16   verification, or biometrics technology (e.g. face recognition),

17   would provide a greater measure of security in ascertaining the

18   identify of the individual actually causing the access event (see

19   discussion below). In a second embodiment involving the user

20   system 21, and denoted by the path indicated by arrow B, the

21   access event can similarly occur upon the activation 25 of an e-

22   mail processing software 23 installed on the user system 21.

23   Alternatively, the access event can occur by opening 26 the

24   delivered e-mail file 12 itself subsequent to activation 25 of

25   the e-mail processing software 23.

1   Upon detecting the access event triggered by the accessing

2   party 20, a series of operations is automatically executed to

3   generate and ultimately transmit a confirmation of receipt notice

4   to the sending party 10. As shown in FIG. 1, this is preferably

5   accomplished by means for generating 27 (preferably including

6   means for informing the accessing party of the delivered e-mail

7   file, and means for discovering recipient data), and means for

8   transmitting 28, both of which are preferably embodied either as

9   modules of a receipt confirmation software 29 installed on the

10   recipient systems 14, 21, or as hardware components 30 also

11   installed on the recipient systems 14, 21. Additionally, in one

12   particular embodiment involving the server-type target system 14,

13   both the means for generating 27 and the means for transmitting

14   28 are installed on the user terminal 19 as either modules of a

15   receipt confirmation software 29 or as hardware components 30.

16   Alternatively, and in another embodiment, the means for

17   generating 27 and means for transmitting 28 (as well as means for

18   informing and means for discovering) are executable modules of an

19   executable attachment file 12' transmitted together with the e-

20   mail file 12. The executable attachment file 12' is preferably a

21   suitably small program capable of self-activating typically by

22   double-clicking the e-mail file 12. The executable attachment

23   file 12' preferably has a module for discovering recipient data

24   associated with the recipient e-mail address, a module for

25   generating the confirmation of receipt notice containing the

19

1   recipient data, and a module for transmitting the confirmation of

2   receipt notice to a return e-mail address designated by the

3   sending party 10 to receive the confirmation of receipt notice.

4   Additionally, where the access event is other than the

5   direct opening of the e-mail file 12, the attachment file 12' may

6   also include a module for detecting the designated access event.

7   The detection module would preferably be executed automatically

8   upon delivery to the recipient e-mail address, in order to

9   immediately wait for and detect the access event. It is

10   appreciated that if opening of the e-mail file 12 is designated

11   as the access event, then directly opening the e-mail file is

12   itself an inherent detection of the access event which does not

13   require a separate detection module. Furthermore, where the

14   access event is again other than the direct opening of the e-mail

15   file 12, the attachment file preferably also includes a module

16   for providing notice of the delivered e-mail to the accessing

17   party 20. Again, it is appreciated that opening of the e-mail

18   file itself will inherently provide notice to the accessing party

19   of the delivery and contents of the e-mail file 12. Generally,

20   however, each of these modules self-execute upon occurrence of

21   the access event, as will be discussed in greater detail of each

22   step.

23   In a preferred embodiment, another executable software

24   module is provided which makes a first determination, prior to

25   the step of detecting the access event, of whether generation and

1 transmission of a confirmation of receipt notice is warranted.

2 The module is preferably resident as part of resident software in

3 the recipient system prior to the delivery of the e-mail file 12.

4 And this determination is preferably made by identifying an e-

5 mail file as a particular file-type requiring a confirmation of

6 receipt notice, and thus requiring a further detection step of

7 the access event. Similar to the discussion above, it is

8 appreciated that if opening of the e-mail file 12 is designated

9 as the access event, then directly opening the e-mail file is

10 itself an inherent detection of the access event which does not

11 require a separate detection module of the resident software of

12 the recipient computer system.

13 E-mail which is designated for generating a confirmation of

14 receipt notice is preferably differentiated from e-mail without

15 such designation by means of the executable attachment file 12'

16 to the e-mail or a distinct file extension of the e-mail. For

17 example, where the e-mail file 12 has an executable attachment

18 file 12', merely accessing that e-mail file 12 will automatically

19 initiate the steps for generating the confirmation of receipt

20 notice (as mentioned above). Additionally, a particular e-mail

21 may be labeled with a distinct file extension to identify the

22 file as one requiring a confirmation of receipt notice. As an

23 illustrative example, the file extension acronym of ".crn"

24 (confirmation of receipt notice) may be used for recognition by

25 the recipient system in order to execute the detection step.

21

1   Turning now to each of the steps which are executed upon

2   detection of the access event 18, 18', 25, 26, arguably one of

3   the most important features of the access event is providing

4   notice of the delivered e-mail to the accessing party 20. While

5   this may be inherently accomplished in the case of opening the

6   delivered e-mail file itself, this is typically not the case for

7   other access events, such as accessing the recipient e-mail

8   address or associated recipient computer 18, 25. These other

9   designated access events may require an additional step of

10   providing sufficient notice because access to the user account 16

11   or the e-mail processing software 23 will not typically notify

12   the presence and/or contents of the e-mail to the accessing party

13   20. This is important because many cases require at least

14   notification of the e-mail delivery to a target party, especially

15   those involving legal documents. In many of those situations,

16   however, the recipient may be unwilling to cooperate with the

17   sending party 10 in returning a confirmation of receipt reply.

18   Therefore, the means for generating 27 shown in FIG. 1 would

19   preferably include means for informing the accessing party 20 of

20   the delivered e-mail 12. It is notable that informing the

21   accessing party 20 would be accomplished either by informing the

22   accessing party 20 of the presence of the e-mail 12, or by

23   opening the e-mail 12 to exhibit the contents of the e-mail,

24   either partially or in its entirety. Moreover, as discussed

25   previously, the executable attachment file 12' may also include a

1   module for providing notice of the delivered e-mail file to the

2   accessing party 20 upon detection of the access event.

3   Additionally, upon detection of the access event 18, 18',

4   25, 26, the system 9 also initiates the step of discovering or

5   otherwise obtaining recipient data, typically from the recipient

6   computer system, for inclusion in a confirmation of receipt

7   notice (see FIGS. 3, 4). It is notable that the discovering

8   steps involves actively searching for recipient data in target

9   locations typically associated with such recipient data, such as

10   for example the recipient system. The discovering step is

11   preferably accomplished in conjunction with the means for

12   generating a confirmation of receipt notice 27, with the

13   generated confirmation of receipt notice having the recipient

14   data contained therein. Moreover, the discovering step includes

15   the compilation of various recipient data associated with the

16   recipient e-mail address, including identity information of a

17   registered user of the recipient e-mail address. Additionally,

18   the recipient data may also include access event data of

19   attendant conditions of the designated access event. The access

20   event data may include, but is not limited to, time and date of

21   access, recipient e-mail address of the account where the e-mail

22   was accessed, geographic address of the location where the access

23   event occurred, telephone number of the location where the access

24   event occurred, data indicating information about the terminal

25   used to trigger the access event (e.g. that the terminal has been

1   activated by a user(s) using a security code such as a password,

2   fingerprint, genetic or retina imprint), and especially the

3   identity of the accessing party 20 (e.g. first and last name,

4   age, date of birth, drivers license number, company name, etc.),

5   etc. Discovering or obtaining the identity of the individual

6   actually causing the access event 18, 18′, 25, 26 would be

7   particularly advantageous where the target party is a business or

8   organizational entity, and employees or other personnel receive

9   important e-mail on its behalf. Such important information can

10   include credit card account information, social security number,

11   confidential memos, business documents such as contracts and

12   bids, and legal documents such as subpoenas, summons and

13   complaint notices, jury duty notices, etc. Moreover,

14   ascertaining the identity of the individual actually causing the

15   access event would provide additional proof of actual receipt of

16   the e-mail 12. For this purpose, it is contemplated that

17   suitable means of identification verification for access known in

18   the relevant art would be used in conjunction with the present

19   invention, such as access upon fingerprint verification, genetic

20   (DNA) verification, retina scan verification, biometrics

21   technology (e.g. face recognition), etc. Such verified

22   identification information is preferably obtained in one

23   embodiment by compiling such information from the recipient

24   computer system or the accessing party's system during the

1   generation of the confirmation of receipt notice as discussed

2   above.

3   In a first preferred embodiment of the discovering step, the

4   system 9 retrieves a pre-recorded recipient data file from the

5   recipient computer system 14, 21 containing pre-recorded

6   recipient data. The pre-recorded recipient data is preferably

7   information associated with a registered user to whom the

8   recipient e-mail address/ account are registered. As discussed

9   previously, the registered user is not necessarily the accessing

10   party 10. The pre-recorded recipient data is typically pre-

11   recorded and resident on the recipient computer system

12   substantially prior to access by the accessing party 20, and

13   often recorded by administrative personnel associated with the

14   management of the recipient e-mail address and account.

15   Additionally, the pre-recorded recipient data may be entered by

16   the registered user at the moment of creation of the recipient

17   account or a similarly early point in time. In any case, upon

18   detecting the access event 18, 18', 25, 26, the pre-recorded

19   recipient data file is retrieved from the recipient computer

20   system for inclusion in the confirmation of receipt notice (see

21   discussion below).

22   FIG. 5 illustrates three sample recipient e-mail addresses/

23   accounts: "mike@aaalawfirm.com" 62, "reubenbahar@server.com" 63,

24   and "xyzcorporation@server.com" 64, all containing e-mail

25   messages delivered to respective recipient computer systems. It

1   is notable that each of the recipient e-mail accounts 62-64 has

2   stored therein a corresponding pre-recorded arrangement of

3   delivery information 65-67, respectively, i.e. the pre-recorded

4   recipient data file relating to the specific user of each of the

5   accounts. As shown, each of the particular pre-recorded

6   arrangements of delivery information 65-67 contains identity data

7   that distinctly identifies the registered recipient party who has

8   proper authorization to access the respective accounts 62-64.

9   Upon detection of the access event on an e-mail for which a

10 confirmation of receipt notice was requested, the pre-recorded

11 recipient data corresponding to a particular user account is

12 discovered for inclusion in the confirmation of receipt notice.

13 For example, detecting access events independently associated

14 with e-mails 68 or 70 will result in retrieval of the pre-

15 recorded recipient data 65 which corresponds to e-mail user

16 account 62. Similarly, triggering an access event associated

17 with e-mail 71 will result in retrieval of the pre-recorded

18 recipient data 66 which corresponds to e-mail user account 63.

19 And finally, an access event associated with e-mail 72 or 73 will

20 result in the retrieval of the pre-recorded recipient data 67

21 which corresponds to e-mail user account 64. It should be

22 mentioned that an access event is not associated with e-mails 69,

23 74, and 75 and will not therefore result in discovery and

24 recording of the pre-recorded recipient data corresponding to the

25 respective user accounts since those e-mails were not designated

1   by the sending party 10 to generate a confirmation of receipt

2   notice message. This is the case since e-mails 69, 74, and 75 do

3   not have a distinct file extension or an executable file

4   attachment which identify the e-mail as a file-type requiring the

5   confirmation of receipt notice.

6   Alternatively, another method of obtaining recipient data,

7   particularly access event data, involves interactively requesting

8   and receiving input from the accessing party 20. In one

9   embodiment, such a step is implemented and required to be

10   completed as a condition for executing the subsequent steps of

11   discovering recipient data, generating the confirmation of

12   receipt notice, and transmitting the confirmation of receipt

13   notice. Thus, for example, when the designated access event is

14   designated as the opening of the e-mail file 12, double-clicking

15   the e-mail file 12 will typically trigger an on-screen request

16   prompting the accessing party to input various information, such

17   as the identity of the accessing party 20. Similarly, when the

18   designated access event is designated as the log-in access of the

19   recipient e-mail address or account, an on-screen request prompts

20   the accessing party 20 to input information in order to gain

21   entry, as well as to execute the subsequent steps of providing

22   notice of the e-mail and generating the confirmation of receipt

23   notice.

24   In a still alternative embodiment, accessing party

25   information is obtained prior to the designated access event as a

27

1   requisite condition for gaining access or entry to a recipient e-

2   mail address or account. Such information requirement is

3   typically implemented via accessing party identifying software

4   which is resident on the recipient computer system 14, 21. The

5   obtained accessing party information is then recorded to an

6   accessing party data file (not shown) for resident storage in the

7   recipient computer system 14, 21. With the accessing party data

8   file resident in the recipient computer system 14, 21, it is

9   retrieved therefrom upon detection of the access event as part of

10   the step of obtaining access event data. A similar process of

11   recording and later retrieving an accessing party data file is

12   implemented where the accessing party 20 remote accesses the

13   recipient e-mail address or account from a remote user computer

14   (e.g. 19 in FIG. 1) which is remote connected to the recipient

15   computer system 14, 21 via the communications network. In this

16   particular embodiment, accessing party information is obtained as

17   a required step to operating the remote user computer, such as is

18   typical of some LAN systems restricted to only authorized

19   persons. Here too a software program resident on the remote user

20   computer is typically utilized to perform the collection of

21   information. The accessing party information is then recorded to

22   an accessing party data file for resident storage in the remote

23   user computer. And upon triggering and detection of the

24   designated access event, the accessing party data file is remote

25   retrieved from the remote user computer.

1   Additionally, in yet another embodiment, information

2   pertaining to the accessing party is obtained by electronically

3   tapping the remote connection in a process known to those skilled

4   in the relevant art (such as that employed in caller

5   identification). Upon the triggering and detection of the access

6   event, an electronic tapping or tracing sequence would

7   automatically initiate through the use of hardware and or

8   software means preferably resident on the recipient computer

9   system 14. It is appreciated that electronic tapping is possible

10   by virtue of the telephone or other communications connection

11   between the recipient computer system 14 and the remote user

12   computer 19, and that the electronic tapping process obtains

13   remote access information associated with the remote connection.

14   It is contemplated that various suitable means for precisely

15   identifying the accessing party known in the relevant art could

16   be used in conjunction with the present invention. These may

17   include, but are not limited to, verification of access based

18   upon fingerprint identification, genetic (DNA) identification,

19   retina scan identification, biometrics technology (e.g. face

20   recognition), or a computer generated user code. Such

21   information may be used in lieu of a password as a means of

22   gaining access to either a computer or online account given its

23   "one of a kind" imprint. Where this information (e.g.

24   fingerprint) is used to gain access to a computer terminal, it is

1   preferably recorded on that terminal's data registry so as to

2   match potential users with authorized ones. Thus, once the e-

3   mail 12 is accessed, the discovery process preferably searches

4   the accessing party's computer registry and retrieves the

5   resident imprint information. Conversely, when imprint

6   information is entered on the spot by a user trying to gain

7   access to e-mail 12, the discovery process preferably detects and

8   record it the moment it is entered. Given the unique signature

9   inherent in one's fingerprint, genetics, retina, and face,

10   acquiring such information virtually ensures the correct

11   identification of the person actually causing the access event.

12   It is noteworthy that in many situations, a user may not

13   want their fingerprint, genetic, retina imprint, or even password

14   revealed to an outside party. In these instances the user's

15   personal security code (e.g. fingerprint, genetic, retina

16   imprint, password) would be associated with the user's identity

17   information, (e.g. name, address, phone number, etc.). For

18   example, a user may input their fingerprint into a computer

19   terminal in order to gain access to that terminal. After the

20   user's fingerprint is recognized by the terminal, the user

21   identity information that is associated with that particular

22   fingerprint will be recorded on the terminal's retrievable data

23   registry instead of the user's fingerprint. Upon the occurrence

24   of an access event, the user information would be retrieved from

1   the terminal's data registry, in accordance with the discovery

2   process. For this process to occur, it is, of course, understood

3   that the user's identity information would have to be pre-

4   programmed into the user terminal and directly associated with

5   the user's personal security code (e.g. fingerprint). Since a

6   particular collection of user identity information would only be

7   responsive to a distinct user security code (e.g. fingerprint),

8   discovery of the user information in this instance would work to

9   positively identify the user of the terminal causing the access

10   event.

11   The discovered and otherwise obtained recipient data and

12   access event data is subsequently included in a confirmation of

13   receipt notice which is preferably generated by a self-executing

14   module upon the detection of the access event, or upon

15   additionally obtaining access event data. As can be seen in

16   FIGS. 3 and 4, two examples of confirmation of receipt notices

17   are shown. In particular, FIG. 3 shows a confirmation of receipt

18   notice 46 which confirms that an e-mail file was delivered to the

19   correct recipient e-mail address 50. The first line 47

20   reiterates the intended target party, e.g. Reuben Bahar 48, and

21   the second line 49 reiterates the intended target e-mail address,

22   e.g. reubenbahar@hotmail.com 50. The third line 51 identifies

23   the recipient e-mail address information, e.g.

24   reubenbahar@hotmail.com 51' which was discovered upon the access

25   event. And the fourth line 52 identifies the identity of the

1   accessing party, e.g. Reuben Bahar 51', who actually received the

2   e-mail file. Thus, the first 47 and fourth 52 lines are compared

3   with each other, and the second 49 and third 51 lines are

4   compared with each other, to determine equivalency. Additional

5   lines of access information, designated at reference character

6   53, is shown providing additional access event data associated

7   with the access event and the accessing party, such as access

8   location, phone number of access location, and the time and date

9   of the access event. Notably, the confirmation of receipt notice

10 46 provides the phone number of the physical location from which

11 the e-mail was accessed, preferably by the electronically tapping

12 process discussed above. And FIG. 4 illustrates a confirmation

13 of receipt notice 54 for an e-mail file which was delivered to a

14 wrong location due to some system or other error. As can be

15 seen, while the first line 55 lists the identity of intended

16 target party, e.g. Reuben Bahar 56, the fourth line 60 indicates

17 that the access event was triggered by a Mike Smith 60'. Further

18 indication is provided of misdirected delivery by comparing the

19 second line 57 of the intended target e-mail address and the

20 third line 59 of the location from which the e-mail was accessed.

21 The additional access event data indicated at reference character

22 61 operates to further confirm that the e-mail was improperly

23 delivered.

24   After the confirmation of receipt notice is generated, it is

25 transmitted to a return e-mail address designated by the sending

32

1   party 10 to receive the confirmation of receipt notice. This is

2   typically accomplished using the means for transmitting 28 in

3   FIG. 1, which can be either an executable module of an e-mail

4   attachment file or a resident program sequence, as discussed

5   earlier. As can be seen in FIG. 1, following the generation of

6   the confirmation of receipt notice 27, the notice is transmitted,

7   by means for transmitting 28, to the sending party 10 at a

8   designated location, typically the sending party's e-mail inbox.

9   And upon receiving the confirmation of receipt notice by the

10   sending party 10, the sending party 10 compares the recipient

11   data and access event data contained therein with intended target

12   information, such as the intended target party and the intended

13   target e-mail address, to ascertain the delivery conditions. A

14   determination is then made whether proper delivery was effected

15   by the e-mail transmission. And in this manner, the discovered

16   and otherwise obtained recipient data or access event data

17   provides evidence of correct or misdirected delivery of the e-

18   mail file 12. Misdirection or improper access would be evident

19   where the actual recipient system or e-mail address differs from

20   the intended target system or e-mail address, or if there was

21   unauthorized access at a properly delivered e-mail destination.

22   FIG. 2 shows a block diagram illustrating a preferred

23   depiction of the method and system 9 discussed above. Starting

24   from the block 31, the sending party acquires an e-mail (not

25   shown in FIG. 2) to send to the recipient party at block 31',

1 either by creating a new e-mail or using an existing e-mail for

2 forwarding. At block 32, the sending party decides whether to

3 utilize the confirmation of receipt system 9 or transmit the e-

4 mail 12 without receipt notification. If the confirmation of

5 receipt notice is not desired, the e-mail 12 is sent by

6 traditional means for e-mail delivery, at block 32", without

7 utilizing the system 9. If a confirmation of receipt notice is

8 desired, the e-mail 12 may be transmitted at block 32' by the

9 sending party 10. If yes, the target system then receives the e-

10 mail at block 33, which simultaneously stores it into the data

11 storage means in block 34.

12 Next, at block 35 the system 9 determines whether the access

13 event occurred which was caused by the recipient party. If not,

14 the e-mail will remain stored until the recipient party accesses

15 the recipient computer system. If yes, at block 36 the system 9

16 determines whether the access event was caused by the recipient

17 party accessing either the server or the e-mail processing

18 software. If yes, information notifying the recipient party of

19 the e-mail's presence is preferably displayed on the screen, as

20 shown in block 37. The display can be a simple notice of the

21 contents and/or title of the e-mail, or a complete opening and

22 viewing of the entire contents. If not, at block 38 the system 9

23 determines whether the access event was caused by the recipient

24 party accessing the delivered e-mail itself. If not, the system

25 9 returns to block 35.

34

1   If so, however, at block 39 the contents of the accessed e-

2   mail is displayed to the accessing party and the system 9

3   generates the confirmation of receipt notice in preparation for

4   delivery to the sending party 10. During this process, delivery

5   information pertaining to the access event is discovered from the

6   recipient computer system, as discussed previously, and included

7   in the confirmation of receipt notice. Block 39 is likewise

8   reached following block 37.

9   At block 40, the system 9 determines whether the manual or

10   automatic transmission option was pre-designated by the sending

11   party. If the automatic transmission option was chosen, the

12   confirmation of receipt notice is automatically transmitted to

13   the sending party 10 at block 44. If the manual transmission

14   option was chosen by the sending party 10, at block 41 the

15   recipient party is prompted whether a confirmation of receipt

16   notice is to be return transmitted to the sending party 10. If

17   at block 41 the recipient party chooses not to transmit the

18   confirmation of receipt notice, the system ends at block 43. If

19   yes, at block 44 the system transmits the confirmation of receipt

20   notice back to the sending party 10, and the sending party 10

21   receives the confirmation of receipt notice at block 45. Upon

22   receiving the confirmation of receipt notice at block 45, the

23   sending party may compare the identity of the accessing party

24   with that of the originally intended target party to determine if

25   delivery of the e-mail was proper. It is notable here that

1   though the above discussion provides a manual transmission option

2   giving the recipient party the choice of not transmitting the

3   confirmation of receipt notice back to the sending party, the

4   sending party will typically have pre-designated the automatic

5   transmission option in order to maintain full control of the

6   return receipt process and ensure the receipt of a confirmation

7   of receipt notice.

8   The present embodiments of this invention are thus to be

9   considered in all respects as illustrative and not restrictive;

10 the scope of the invention being indicated by the appended claims

11 rather than by the foregoing description. All changes which come

12 within the meaning and range of equivalency of the claims are

13 intended to be embraced therein.